

(19)日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-190667

(43)公開日 平成9年(1997)7月22日

| (51)Int.Cl. <sup>6</sup> | 識別記号  | 庁内整理番号 | F I           | 技術表示箇所  |
|--------------------------|-------|--------|---------------|---------|
| G 1 1 B 19/02            | 5 0 1 |        | G 1 1 B 19/02 | 5 0 1 Q |
| G 0 6 F 12/14            | 3 2 0 |        | G 0 6 F 12/14 | 3 2 0 B |

審査請求 未請求 請求項の数44 O L (全 17 頁) 付 5

(21)出願番号 特願平8-985

(22)出願日 平成8年(1996)1月8日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 中村 誠一

東京都青梅市末広町2丁目9番地 株式会

社東芝青梅工場内

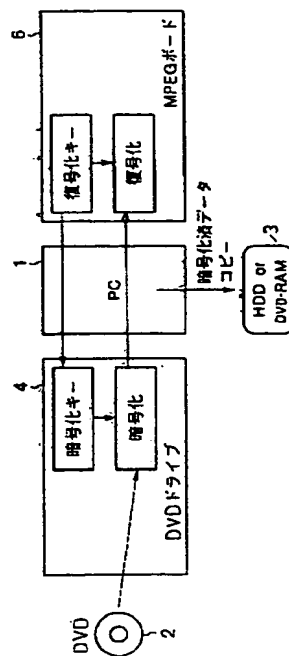
(74)代理人 弁理士 鈴江 武彦

(54)【発明の名称】 複製制御方法及び複製制御装置

## (57)【要約】

【課題】本発明は、ドライブから情報伝達手段に受け渡される情報を、情報再生装置で生成したキー情報を用いて暗号化処理し、暗号化処理に用いたキー情報をもつ情報再生装置のみがドライブで読出した情報を複製し再生できるようにして、大容量記録媒体、通信媒体等の媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能なシステムが構築できることを特徴とする。

【解決手段】MPEGボード6は当該ボードで生成したキー情報をDVDドライブ4に発行する。DVDドライブ4は上記キー情報をもとにして暗号化キー情報を生成し、当該キー情報によりDVD2より読出された提供情報を暗号化処理し、MPEGボード6に送出する。MPEGボード6は当該ボードで生成したキー情報を用いて暗号化処理された提供情報を復号化処理する。



1

## 【特許請求の範囲】

【請求項1】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置として記録できる手段とを備えたシステムに於いて、

ドライブは、情報再生装置よりキー情報を受け、当該キー情報をもとに大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に渡し、

情報再生装置は、情報伝達手段から受けた暗号化処理された情報をドライブに発行したキー情報に関連するキー情報により復号化処理して再生できることを特徴とした大容量記録媒体に記録された情報の複製制御方法。

【請求項2】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を記録できる手段とを備えたシステムに於いて、

情報再生装置がドライブにキー情報を発行し、ドライブが情報再生装置より受けたキー情報をもとに大容量記録媒体より読出した情報を暗号化処理し情報伝達手段に渡して、

ドライブにキー情報を発行した情報再生装置のみが情報伝達手段を介して記録した情報を復号化処理して再生できることを特徴とした大容量記録媒体に記録された情報の複製制御方法。

【請求項3】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブと情報再生装置がランダムな情報を用いて互いに関連するキー情報を一時的に生成し、

ドライブが、自己生成した一時的なキー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した一時的なキー情報を用いて情報伝達手段より受けた情報を復号化して、

ドライブより読出した情報の再生を可能にし、ドライブより読出した情報を一旦記録した複製情報の再生を不可にしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。

【請求項4】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

少なくともドライブ又は情報再生装置が、ランダムな情報をもとに一次キー情報を生成し、当該キー情報をもとにしてドライブ及び情報再生装置がそれぞれ一時的な二次キー情報を自己生成し、

ドライブが、自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受け

2

た情報を復号化することにより、

ドライブより読出された情報の再生を可能にし、複製情報の再生を不可にしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。

【請求項5】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブ及び情報再生装置のそれぞれが、ランダムな情報をもとに一次キー情報を生成し、当該キー情報を相互に受け渡し、その各一次キー情報をもとにして一時的な二次キー情報を自己生成し、

ドライブが、自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することにより、

暗号化及び復号化に供されるキー情報を情報伝達手段から隠して、複製情報の再生を不可にしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。

【請求項6】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブは、大容量記録媒体より、再生の対象となる情報の読出しに際して、特定の制御情報を読み、その制御情報から、当該記録媒体より読出され一旦記録された複製情報に対しての複製許可レベルを認識して、

複製許可レベルが特定の情報再生装置でのみ複製情報の再生を許可するレベルであるとき、再生を行なう情報再生装置よりキーのもとになる情報を受け、当該情報をもとに生成したキー情報により、大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に受け渡し、

複製許可レベルが全ての情報再生装置での複製情報の再生を禁止するレベルであるとき、再生を行なう情報再生装置よりランダムな情報を受け、当該情報をもとに一時的なキー情報を生成して、当該キー情報により大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に受け渡して、

大容量記録媒体に記録した特定の制御情報により、複製情報の複製許可を任意にコントロールできるようにしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。

【請求項7】 情報伝達手段は、コンピュータ装置又は情報伝送装置又は伝送する情報の記録が可能な他の装置により実現される請求項1又は2又は3又は4又は5又は6記載の複製制御方法。

【請求項8】 情報再生装置は、MPEG1又はMPEG2又はMPEG4を対象としたMPEGデコーダを搭載した再生ボードにより実現される請求項1又は2又は3又は4又は5又は6記載の複製制御方法。

【請求項 9】 大容量記録媒体は、MPEG 1又はMPEG 2又はMPEG 4で圧縮された映像情報を含む提供情報を固定記録したディスクにより実現される請求項 1又は2又は3又は4又は5又は6記載の複製制御方法。

【請求項 10】 情報再生装置で生成したキー情報を複製情報に対応付けて保存する手段をもつ請求項 1又は2又は3記載の複製制御方法。

【請求項 11】 任意の値をもつキー情報を設定できる請求項 1又は2又は3記載の複製制御方法。

【請求項 12】 少なくとも暗号化又は復号化の処理に用いられるキー情報は、少なくとも再生の開始又は終了の都度、内容が変更される1又は2又は3又は4又は5又は6記載の複製制御方法。

【請求項 13】 情報再生装置は、互いに関連付けされた暗号化のキー情報及び復号化のキー情報をもち、少なくとも暗号化のキー情報を暗号化処理してドライブに送出する手段をもつ請求項 1又は2記載の複製制御方法。

【請求項 14】 大容量記録媒体より読出される特定の制御情報の内容が変る度に、少なくとも暗号化又は復号化の処理に用いられるキー情報の内容が変更される請求項 6記載の複製制御方法。

【請求項 15】 ドライブと情報再生装置との間で受け渡されるキー情報が情報伝達手段上に於いて暗号化処理される請求項 1又は3又は4又は5又は6記載の複製制御方法。

【請求項 16】 大容量記録媒体に記録されドライブ装置で読出された情報を受けて再生処理するデコーダを備えた情報再生装置に於いて、ドライブより受けた情報を復号化するためのキー情報を内部に発行し、ドライブより出力される情報を暗号化するためのキー情報をドライブに発行する手段を設けてなることを特徴とした大容量記録媒体の情報再生装置。

【請求項 17】 大容量記録媒体に記録された情報を読出して情報再生装置に受け渡す大容量記録媒体のドライブ装置に於いて、大容量記録媒体に記録された情報を再生する際に情報再生装置よりキー情報を受けて保持する手段と、このキー情報をもとにして情報再生装置へ転送する情報を暗号化する手段とを具備してなることを特徴とする大容量記録媒体のドライブ装置。

【請求項 18】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を複製情報として記録できる手段とを備えたシステムに於いて、情報再生装置に、キー情報の生成手段、及びキー情報をドライブに発行する手段を設け、ドライブに、上記キー情報を受け、このキー情報をもとに大容量記録媒体から読出した情報を暗号化処理する手段を設けて、ドライブにキー情報を発行した情報再生装置のみが複製

情報を再生できることを特徴とする複製制御装置。

【請求項 19】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブ及び情報再生装置に、互いに関連する情報で個別にキー情報を生成する手段を設け、

ドライブに、自己生成したキー情報を用いて、情報伝達手段に出力する情報を暗号化する手段を設け、

10 情報再生装置に、自己生成したキー情報を用いて、情報伝達手段より受けた情報を復号化する手段を設けて、

暗号化及び復号化に用いるキー情報を情報伝達手段より隠したことを特徴とする大容量記録媒体に記録された情報の複製制御装置。

【請求項 20】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

少なくともドライブ又は情報再生装置に、ランダムな情報をもとに一次キー情報を生成する手段を設け、

20 ドライブ及び情報再生装置に、上記一次キー情報をもとにして一時的な二次キー情報を自己生成する手段を設けて、

ドライブが、自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することを特徴とした複製制御装置。

【請求項 21】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、

ドライブ及び情報再生装置のそれぞれに、ランダムな情報をもとに一次キー情報を生成する手段と、その双方で生成された各一次キー情報を用いて二次キー情報を生成する手段とを設け、

ドライブが自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することを特徴とする複製制御装置。

40 【請求項 22】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を複製情報として記録できる手段とを備えたシステムに於いて、

ドライブ及び情報再生装置に、相互に関連するキー情報を保持する手段と、大容量記録媒体に記録された特定の制御情報を受けて、大容量記録媒体から読出される情報の複製許可レベルを判断する手段とを設け、

ドライブに、複製許可レベルに応じて、大容量記録媒体より読出した情報を、関連するキー情報をもつ情報再生

装置でのみ複製情報を復号処理できるように暗号化処理し、又は全ての情報再生装置が複製情報を復号処理できないように暗号化処理し、又は暗号化処理を施さずに情報伝達手段に受け渡す手段とを設けて、大容量記録媒体に記録された特定の制御情報により、複製情報の複製許可を任意にコントロールできるようにしたことを特徴とする複製制御装置。

【請求項 2 3】 情報再生装置に、キー情報の生成手段、及びキー情報をドライブに発行する手段を設け、ドライブに、上記キー情報を受け、このキー情報をもとに大容量記録媒体から読出した情報を暗号化処理する手段を設けて、複製情報の再生を特定の情報再生装置でのみ可能とした請求項 2 2 記載の複製制御装置。

【請求項 2 4】 ドライブ及び情報再生装置に、互いに関連する情報で個別にキー情報を生成する手段を設け、ドライブに、自己生成したキー情報を用いて、情報伝達手段に出力する情報を暗号化する手段を設け、情報再生装置に、自己生成したキー情報を用いて、情報伝達手段より受けた情報を復号化する手段を設けて、全ての情報再生装置が複製情報を復号処理できないようにした請求項 2 2 記載の複製制御装置。

【請求項 2 5】 情報伝達手段は、コンピュータ装置又は情報伝送装置又は伝送する情報の記録が可能な他の装置により実現される請求項 1 8 又は 1 9 又は 2 0 又は 2 1 又は 2 2 又は 2 3 記載の複製制御装置。

【請求項 2 6】 情報再生装置は、MPEG 1 又は MPEG 2 又は MPEG 4 を対象とした MPEG デコーダを搭載したボードにより実現される請求項 1 8 又は 1 9 又は 2 0 又は 2 1 又は 2 2 又は 2 3 記載の複製制御装置。

【請求項 2 7】 大容量記録媒体は MPEG 1 又は MPEG 2 又は MPEG 4 で圧縮された映像情報を含む提供情報を固定記録したディスクにより実現される請求項 1 8 又は 1 9 又は 2 0 又は 2 1 又は 2 2 又は 2 3 又は 2 4 記載の複製制御装置。

【請求項 2 8】 情報再生装置で生成したキー情報を複製情報に対応付けて保存する手段をもつ請求項 1 8 又は 2 2 又は 2 3 記載の複製制御装置。

【請求項 2 9】 任意の値をもつキー情報を設定できる請求項 1 8 又は 2 2 又は 2 3 記載の複製制御装置。

【請求項 3 0】 少なくとも暗号化又は復号化の処理に用いられるキー情報は、少なくとも再生の開始又は終了の都度、内容が変更される請求項 1 8 又は 1 9 又は 2 0 又は 2 1 又は 2 2 又は 2 3 又は 2 4 記載の複製制御装置。

【請求項 3 1】 情報再生装置は、互に関連付けされた暗号化のキー情報及び復号化のキー情報を持ち、少なくとも暗号化のキー情報を暗号化処理してドライブに送出する手段をもつ請求項 1 8 又は 2 2 記載の複製制御装置。

【請求項 3 2】 大容量記録媒体より読出される特定の

制御情報の内容が変る度に、少なくとも暗号化又は復号化の処理に用いられるキー情報の内容が変更される請求項 2 2 又は 2 3 又は 2 4 記載の複製制御装置。

【請求項 3 3】 ドライブと情報再生装置との間で受け渡されるキー情報が情報伝達手段上に於いて暗号化処理される請求項 1 8 又は 2 0 又は 2 1 又は 2 2 記載の複製制御装置。

【請求項 3 4】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えてなるシステムに於いて、情報再生装置が情報提供装置にキー情報を発行し、情報提供装置が情報再生装置より受けたキー情報をもとに提供先の情報再生装置に送信する情報を暗号化処理して、暗号化処理に用いられたキー情報を発行した情報再生装置のみが複製情報を再生できることを特徴とする通信により提供される情報の複製制御方法。

【請求項 3 5】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、情報提供装置と情報再生装置がランダムな情報を用いて互に関連するキー情報を一時的に生成し、情報提供装置が自己生成した一時的なキー情報を用いて通信手段に送出する情報を暗号化し、情報再生装置が自己生成した一時的なキー情報を用いて通信手段を介して受けた情報を復号化して、

通信手段を介して受けた情報の再生を可能にし、当該情報を一旦記録した複製情報の再生を不可にしたことを特徴とする通信により提供される情報の複製制御方法。

【請求項 3 6】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、

情報提供装置は、複製情報の許可レベルを指定する複製許可情報を情報再生装置に送出し、

情報再生装置は、情報提供装置より受けた複製許可情報をもとに、提供される情報の複製の許可レベルを認識して、

複製情報の再生が可能な許可レベルであるときは、提供される情報を暗号化処理せずに通信手段を介して情報再生装置に受け渡し、

複製情報の再生が特定の情報再生装置でのみ可能な許可レベルであるときは、情報再生装置よりキー情報を受け、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡し、

複製情報の再生を禁止する許可レベルであるときは、情

報提供装置及び情報再生装置がランダムな情報を用いて互いに関連するキー情報を一時的に生成し、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡すことを特徴とする通信により提供される情報の複製制御方法。

【請求項37】 通信手段は、コンピュータ装置と当該装置に接続される通信回線とにより実現される請求項34又は35又は36記載の通信により提供される情報の複製制御方法。

【請求項38】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、  
情報再生装置に、当該装置に固有のキー情報を生成する手段を設け、  
情報提供装置に、情報再生装置よりキー情報を受け、当該キー情報をもとに提供情報を暗号化処理する手段を設けて、  
暗号化処理に供されたキー情報をもつ情報再生装置のみが複製情報を再生できることを特徴とする通信により提供される情報の複製制御装置。

【請求項39】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、  
情報提供装置及び情報再生装置のそれぞれに、互いに関連する情報で個別にキー情報を生成する手段する手段を設け、  
情報提供装置が自己生成したキー情報を用いて通信手段に送出する提供情報を暗号化処理し、情報再生装置が自己生成した情報を用いて通信手段を介して受けた情報を復号化することを特徴とする通信により提供される情報の複製制御装置。

【請求項40】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、  
情報提供装置に、情報提供に際して当該情報の複製許可レベルを認識する手段と、複製許可情報が複製情報の再生を許可するレベルであるとき、提供する情報を暗号化処理せずに通信手段を介して情報再生装置に受け渡す手段と、

複製許可情報が、複製情報の再生を特定の情報再生装置のみ許可するレベルであるとき、再生を行なう情報再生装置が生成したキー情報を受け、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介して情報再生装置に受け渡し、

複製許可情報が、複製情報の再生を許可しないレベルであるときは、再生を行なう情報再生装置よりランダムな情報を受け、当該情報をもとに一時的なキー情報を生成して、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介して情報再生装置に受け渡すことを特徴とする通信により提供される情報の複製制御装置。

【請求項41】 通信手段は、通信回線、及び当該回線に回線接続されたコンピュータ装置により実現される請求項38又は39又は40記載の通信により提供される情報の複製制御装置。

【請求項42】 情報再生装置はMPEG1又はMPEG2又はMPEG4を対象としたMPEGデコーダを搭載したボードにより実現される請求項38又は39又は40又は41記載の通信により提供される情報の複製制御装置。

【請求項43】 情報提供装置はMPEG1又はMPEG2又はMPEG4で圧縮された映像情報を含む提供情報を通信手段を介し情報再生装置に送信する請求項38又は39又は40記載の通信により提供される情報の複製制御装置。

【請求項44】 映像情報を含む提供情報を記録した媒体から情報を読み出す読出装置と、この読出装置に接続されるコンピュータ装置と、このコンピュータ装置で受取った提供情報を再生処理するボードと、コンピュータ装置に渡された情報を複製情報として記録できる手段とを備えたコンピュータシステムであって、  
読出装置には、乱数により任意の第1のキー情報を発生する手段と、第1のキー情報を保持する手段と、ボードより第2のキー情報を受けて保持する手段と、第1のキー情報と第2のキー情報から第3のキー情報を生成する手段と、ボードよりボードに固有の暗号化された第5のキー情報を受け第3のキー情報により復号化して保持する手段と、第1のキー情報をボードに送出する手段と、  
媒体から複製許可情報を読み出し保持する手段と、複製許可情報に従い第3のキー情報又は第5のキー情報を用いて媒体から読出した提供情報を選択的に暗号化処理する手段とを具備し、

ボードには、乱数により任意の第2のキー情報を発生する手段と、第2のキー情報を保持する手段と、第2のキー情報を読出装置に送出する手段と、読出装置より第1のキー情報を受けて保持する手段と、第1のキー情報と第2のキー情報から第4のキー情報を生成する手段と、  
ボードに固有の第5、第6のキー情報を発生する手段と、第5のキー情報を第4のキー情報を用いて暗号化し読出装置に送出する手段と、読出装置から複製許可情報を受けて保持する手段と、複製許可情報に従い第4のキー情報又は第6のキー情報を用いてコンピュータ装置より受けた提供情報を選択的に復号化処理する手段とを具備し、

50 第5のキー情報を用いて暗号化処理し、第6のキー情報

を用いて復号化処理したとき、当該各キー情報を発行したボードのみが、媒体より読出した情報の複製情報を再生可能にし、第3のキー情報を用いて暗号化処理し、第4のキー情報を用いて復号化処理したとき、媒体より読出した情報の再生を可能にし、複製情報の再生を不可にすることを特徴とした複製制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばMPEG2等により圧縮処理された映画、音楽等の情報（提供情報と称す）を再生出力する提供情報の再生機能をもつ情報処理システムに適用される複製制御方法及び複製制御装置に関する。

【0002】本発明は、例えばCD-ROM、DVD（デジタルビデオディスク）等の大容量記録媒体に記録された情報を複製情報として記録し再生する際の複製情報の再生利用を当該媒体に記録された特定の制御情報によりコントロールできる複製制御方法及び複製制御装置に関する。

【0003】本発明は、通信手段を介して映画、音楽等の提供情報を受信し、当該提供情報を再生出力する機能を備えたコンピュータシステムに適用される、通信により提供される情報の複製制御方法及び複製制御装置に関する。

【0004】

【従来の技術】映画産業や音楽産業から提供される、例えばMPEG2等により圧縮処理された、映画、音楽等の情報（提供情報と称す）を再生出力するシステムに於いては、不正な複製を防止するためのコピープロテクト技術が必要とされる。

【0005】特に、上記したような付加価値の高い提供情報をコンピュータ処理して再生出力するシステムに於いては、コンピュータ処理で解除されてしまう程度のコピープロテクト技術ではなく、不正な複製を確実に防止することのできる信頼性の高いコピープロテクト技術の確立が必要不可欠とされる。

【0006】従来のこの種コピープロテクト技術は、提供情報を記録したCD-ROM等の記録媒体に、不正複製防止情報を併せて記録しておき、この不正複製防止情報を提供情報とともに読出して不正複製防止装置に伝送し、提供情報に複製防止の加工を施すことにより不正複製を防止している。

【0007】しかしながら、このような従来のコピープロテクト技術に於いては、ディスクに記録されている提供情報が不正複製防止装置に伝送されるまで複製防止の加工が施されておらず、従ってディスクの読出装置と再生装置との間に伝送装置としてコンピュータ装置が介在するようなシステム構成に於いては提供情報の故意の不正複製を許してしまう。

【0008】このように、従来では、提供情報の受け渡しにコンピュータが介在するシステムに於いて、不正な複製を確実に防止することのできる信頼性の高いコピープロテクト技術が確立されておらず、特に、提供情報の一部を選択的にコンピュータに取り込んで利用できるシステムを構築しようとしたとき、全ての提供情報を対象に不正な複製を許してしまうという問題があった。

【0009】

【発明が解決しようとする課題】上述したように、従来では、大容量記録媒体等により提供される映画情報、音楽情報等の提供情報の受け渡しにコンピュータが介在するシステムに於いて、不正な複製を確実に防止することのできる信頼性の高いコピープロテクト技術が確立されておらず、特に、提供情報の一部を選択的にコンピュータに取り込んで利用できるシステムを構築しようとしたとき、全ての提供情報を対象に不正な複製を許してしまうという問題があった。

【0010】本発明は上記実情に鑑みなされたもので、大容量記録媒体等により提供される情報の受け渡しにコンピュータが介在するシステムに於いても、不正な複製を確実に防止することのできる信頼性の高い複製制御方法及び複製制御装置を提供することを目的とする。

【0011】又、本発明に於いては、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ装置が介在するシステムに於いても、コンピュータ装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能な複製制御方法及び複製制御装置を提供することを目的とする。

【0012】

【課題を解決するための手段】本発明は、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステムに於いて、コンピュータ等の複製処理が可能な装置上では、媒体より読出された情報が特定のキーにより暗号化された状態であるため、複製情報の再生可否を任意にコントロールできる。

【0013】又、本発明は、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステムに於いて、コンピュータ等の複製処理が可能な装置に、暗号化及び復号化の処理に用いるキー情報を直接見せずに、媒体側で提供情報毎に複製情報の再生利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製の再生による提供情報の活用が可能な複製制御方法及び複製制御装置を提供する。尚、本発明に於いては、大容量記録媒体、通信媒体等により提供される情報を記憶装置等に一旦記録し、読出して再生することを「複製情報の再生」と称している。

【0014】即ち、本発明は、大容量記録媒体に記録された情報を読み出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を複製情報として記録できる手段とを備えたシステムに於いて、ドライブから情報伝達手段に受け渡される情報を、情報再生装置で生成したキー情報を用いて暗号化処理し、暗号化処理に用いたキー情報をもつ情報再生装置のみが複製情報を再生できる（即ち一代コピーを許可する）ことを特徴とする。

【0015】又、上記システムに於いて、ドライブ及び情報再生装置のそれぞれが、ランダムな情報をもとに互に関連するキー情報を個別に生成し、ドライブが、自己生成したキー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することにより、暗号処理及び復号処理に用いたキー情報を情報伝達手段に渡すことなく、関連するキー情報をもつ情報再生装置のみの再生を許可し、複製情報の再生を不可にすることを特徴とする。

【0016】又、上記システムに於いて、ドライブ及び情報再生装置が、大容量記録媒体に記録された特定の制御情報をもとに、複製許可レベルを認識し、複製情報の再生を許可するレベルであるときは、ドライブより読出した情報を暗号化処理せずに情報伝達手段に受け渡し、複製情報の再生を特定の情報再生装置でのみ許可するレベルであるときは、ドライブより読出した情報を、再生を行なう情報再生装置で生成したキー情報を用いてドライブより読出した情報を暗号化処理した後、情報伝達手段に受け渡し、複製情報の再生を禁止するレベルであるときは、ドライブと情報再生装置がランダムな情報を用いて互に関連するキー情報を一時的に生成して、関連するキー情報をもつ情報再生装置のみドライブより読出した情報の再生を可能にし、関連するキー情報をもつ情報再生装置を含む全ての情報再生装置の複製情報の再生を不可にしたことを特徴とする。

【0017】又、本発明は、通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステムに於いて、情報提供装置が情報再生装置よりキー情報を受け、当該キー情報をもとにして情報再生装置に提供する情報を暗号化処理し、暗号化処理に用いたキー情報をもつ情報再生装置のみが複製情報を再生できることを特徴とする。

【0018】又、上記システムに於いて、情報提供装置及び情報再生装置のそれぞれが、ランダムな情報をもとに互に関連するキー情報を個別に生成し、情報提供装置が自己生成した暗号化キー情報を用いて情報再生装置に提供する情報を暗号化し、情報再生装置が自己生成し

た復号化キー情報を用いて情報提供装置より受けた情報を復号化することにより、通信手段を介して受けた情報の再生を可能にし、複製情報の再生を不可にしたことを特徴とする。

【0019】又、上記システムに於いて、情報提供装置は、複製情報の許可レベルを指定する複製許可情報を情報再生装置に送出し、情報再生装置は、情報提供装置より受けた複製許可情報をもとに、提供される情報の複製の許可レベルを認識して、複製情報の再生が可能な許可レベルであるときは、提供する情報を暗号化処理せずに通信手段を介して情報再生装置に受け渡し、複製情報の再生が特定の情報再生装置でのみ可能な許可レベルであるときは、情報再生装置よりキー情報を受け、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡し、複製情報の再生を禁止する許可レベルであるときは、情報提供装置及び情報再生装置がランダムな情報を用いて互に関連するキー情報を一時的に生成し、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡すことを特徴とする。

【0020】上記したような複製制御機構をもつことにより、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステムに於いても、コンピュータ等の複製処理が可能な装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製情報の再生を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能なシステムが構築できる。

【0021】

【発明の実施の形態】以下図面を参照して本発明の実施形態を説明する。図1は本発明の第1の実施形態に於ける基本的なシステム構成を示すブロック図であり、ここでは、大容量記憶媒体（DVD2）に記録された、映画、音楽等の提供情報を複製防止の対象として、ドライブ（DVDドライブ4）から情報伝達手段（PC1）に受け渡される提供情報を、情報再生装置（MPEGボード6）内で生成したキー情報を用いて暗号化処理することで、暗号化処理したキー情報をもつ情報再生装置（MPEGボード6）のみがドライブ（DVDドライブ4）で読出した情報を複製し再生できる、一代コピーを許可する実施形態を例示している。

【0022】図1に於いて、1はドライブで読取った提供情報を情報再生装置に受け渡す情報伝達手段となるコンピュータ装置（PC）であり、ここではドライブで読取った複製許可された提供情報を選択的に取り込み、HDD、DVD-RAM等の外部記憶装置3に記憶して、編集、校正等の処理を可能とする。

【0023】2は複製制御の対象となる映画、音楽等の提供情報を記録したDVDディスクである。このDVD

2には、上記提供情報が例えばMPEG2により圧縮処理して記録されるとともに、この提供情報に対応して、メディア・ファイル管理情報ブロックの一部に、図7に示すような複製許可情報(CGMS)が記録される。

【0024】4はDVD2の情報を読取るドライブ装置であり、ここではDVDドライブと称している。このDVDドライブ4は、情報再生装置内で生成したキー情報を受け、当該キー情報を用いて、DVD2より読取った提供情報を暗号化処理する機能をもつ。この機能の具体的な構成例は図2に示される。

【0025】6はDVDドライブ4で読取った提供情報をコンピュータ装置(PC)1を介して受け再生出力処理する情報再生装置であり、ここではMPEGボードと称している。このMPEGボード6は、MPEG2デコーダを搭載し、コンピュータ装置(PC)1を介して受けた、MPEG2により圧縮処理された提供情報をデコードして再生出力情報を得る。更にこのMPEGボード6には、キー情報を生成し、そのキー情報をDVDドライブ4に送出するとともに、そのキー情報を用いて提供情報を復号化処理する機能をもつ。この機能の具体的な構成例は図2に示される。

【0026】上記図1の構成に於いて、MPEGボード6は当該ボード6で生成したキー情報をDVDドライブ4に発行するとともに、当該キー情報を復号化キーとして保持する。

【0027】DVDドライブ4は上記キー情報を用いて暗号化キーを生成し、当該キーを用いて、DVD2より読出された提供情報を暗号化処理した後、コンピュータ装置(PC)1を介しMPEGボード6に送出する。

【0028】MPEGボード6はDVDドライブ4より暗号化された提供情報をコンピュータ装置(PC)1を介して受け、当該ボードで生成した復号化キーを用いて復号化処理する。

【0029】このような複製制御機構を備えることにより、暗号化処理に用いたキー情報をもつMPEGボード6のみがDVDドライブ4で読出した情報を複製情報として記録して再生できる。

【0030】即ち、DVDドライブ4が、1種類(又は一つ)の提供情報に対して、1種類の暗号化を施せば、情報伝送装置を介して複数の情報再生装置が接続されていても、暗号化に供されたキー情報をもつ情報再生装置以外は複製情報の再生利用が不可能となる。

【0031】尚、具体的な構成では、MPEGボード6からDVDドライブ4に送られるキー情報には暗号化処理が施される。又、具体的な構成では、上記実施形態による複製の排他制御が上記複製許可情報(CGMS)により選択的に有効となるもので、具体例を挙げると、図7に於いて、CGMSのb0、b1が“01”であるとき、上記した複製の排他制御が可能となる。

【0032】図2は本発明の第2の実施形態に於けるシ

ステム構成を示すブロック図であり、ここでは、大容量記録媒体に記録された複製許可情報(CGMS)に従い、ドライブより読出された提供情報を一旦記録した複製情報の再生をすべての情報再生装置に対して可能にするコピーフリーの複製許可レベルと、上記複製情報の再生を特定の情報再生装置でのみ可能にする許可レベルと、上記複製情報の再生をすべての情報再生装置に対して許可しない許可レベルとを選択的に切り替える機能をもつシステムを実現している。

10 【0033】図2に於いて、10及び10Aは図1に示すコンピュータ装置(PC)1に相当するもので、10はシステム全体の制御を司るコンピュータ本体のCPU、10Aは同システムバスである。ここではCPU10の制御の下に、図3乃至図6に示すような複製制御処理が実行される。又、CPU10は、ドライブ装置40が情報記録媒体20より読取った複製許可された提供情報を選択的に取り込み、記憶装置30に記憶して、編集、校正等の処理を可能とする。

20 【0034】20は図1に示すDVD2に相当する情報記録媒体であり、ここではMPEG2により圧縮処理して記録されるとともに、この提供情報に対応して、メディア・ファイル管理情報ブロックの一部に、図7に示すような複製許可情報(CGMS)が記録される。

30 【0035】30は図1に示す外部記憶装置3に相当する記憶装置であり、ここでは複製情報の保存、編集、校正等に供される。40は図1に示すDVDドライブ4に相当するドライブ装置であり、情報記録媒体20の情報を読取る。ここでは、暗号生成装置41、44、暗号キーを貯えるレジスタ42、43、45、48、51、読出装置46、暗号化装置47、49、復号化装置50等を備えて構成される。

【0036】暗号生成装置41は、乱数発生装置を用いたランダムな値をもとに暗号キー(1)を発生する。レジスタ42は暗号発生装置41が発生した暗号キー(1)を保持する。レジスタ43はシステムバス10Aを介して再生装置60より受けた暗号キー(2)を保持する。

40 【0037】暗号生成装置44は暗号キー(1)と暗号キー(2)とを用いて暗号キー(3)を生成する。レジスタ45は暗号発生装置44が発生した暗号キー(3)を保持する。

【0038】読出装置46は情報記録媒体20に記録された情報を読出す。ここでは複製制御の対象となる映画、音楽等の提供情報、及び当該提供情報の複製許可レベルを示す図7に示すような複製許可情報(CGMS)それぞれを読出す。

50 【0039】暗号化装置47は、情報記録媒体20より読出した提供情報を複製許可情報(CGMS)に従い、レジスタ45に貯えられた暗号キー(3)、又はレジスタ51に貯えられた提供情報暗号化キー(5)を用いて



暗号化処理し、又は暗号化処理を施さずに、システムバス10Aを介して再生装置60に送出する。

【0040】レジスタ48は情報記録媒体20より読み取った複製許可情報(CGMS)を保持する。暗号化装置49はレジスタ48に貯えられた複製許可情報(CGMS)を暗号化処理してシステムバス10Aを介し再生装置60に送出する。

【0041】復号化装置50は再生装置60より受けた、暗号化処理された装置固有の提供情報暗号化キー(5)を復号化する。レジスタ51は復号化装置50で復号化処理された暗号化キー(5)を保持する。

【0042】60は図1に示すMPEGボード6に相当する提供情報の再生装置であり、MPEGデコーダを搭載し、システムバス10Aを介して受けた、MPEG2により圧縮処理された提供情報をデコードして再生出力情報を得る。ここでは、暗号生成装置61、64、暗号キーを貯えるレジスタ62、63、65、69、71、72、復号化装置66、67、MPEG2デコーダ68、暗号化装置70等を備えて構成される。

【0043】暗号生成装置61は、乱数発生装置を用いたランダムな値をもとに暗号キー(2)を発生する。レジスタ62はシステムバス10Aを介してドライブ装置40より受けた暗号キー(1)を保持する。レジスタ63は暗号生成装置61で発生した暗号キー(2)を保持する。

【0044】暗号生成装置64は暗号キー(1)と暗号キー(2)とを用いて暗号キー(4)を生成する。レジスタ65は暗号発生装置64が発生した暗号キー(4)を保持する。

【0045】復号化装置66は、コンピュータ本体のシステムバス10Aを介してドライブ装置40より受けた、暗号化処理された複製許可情報(CGMS)を復号化する。

【0046】復号化装置67はコンピュータ本体のシステムバス10Aを介してドライブ装置40より受けた提供情報を、レジスタ71に貯えられた複製許可情報(CGMS)に従い、レジスタ65に貯えられた暗号キー(4)、又はレジスタ72に貯えられた提供情報復号化キー(6)を用いて復号化処理し、又は復号化処理を施さずに、MPEG2デコーダ68に送出する。

【0047】MPEG2デコーダ68は、復号化装置67で復号化した提供情報をデコード処理して再生出力可能な提供情報を表示コントローラ80に送出する。レジスタ69は装置固有の提供情報暗号化キー(5)を保持する。暗号化装置70はレジスタ69に貯えられた装置固有の提供情報暗号化キー(5)を暗号化処理してドライブ装置40に送出する。

【0048】レジスタ71は復号化装置66で復号化された複製許可情報(CGMS)を保持する。レジスタ72はレジスタ69に貯えられた装置固有の提供情報暗号

化キー(5)と対をなす(例えば値が共通する)提供情報復号化キー(6)を保持する。

【0049】80はMPEG2デコーダ68より出力された提供情報を表示装置81に表示出力する表示コントローラである。尚、レジスタ45、65のキー値は、少なくとも再生の開始時又は終了時に一旦クリアされて書き替えられる。又、レジスタ69、72のキー値も、固定値のみでなく、例えば、再生の開始時等に関し書き替える構成であってもよい。

【0050】図3乃至図6はそれぞれ本発明の第2実施形態に於ける処理手順を示すフローチャートであり、このうち、図3及び図4はそれぞれ暗号化及び復号化処理のための各種キー情報の設定処理手順を示すフローチャート、図5及び図6はそれぞれ提供情報読出し時に於ける複製制御処理手順を示すフローチャートである。

【0051】図7は情報記録媒体20に記録されたメディア・ファイル管理情報ブロック内の複製許可情報(CGMS)を説明するための情報フォーマットを示す図である。ここでは、CGMSのb0、b1が“00”であるとき、全ての再生装置60に対して複製情報の再生を許可し、b0、b1が“01”であるとき、提供情報読出し時に利用された再生装置のみに対して排他的な複製情報の再生を許可し、b0、b1が“11”であるとき、全ての再生装置60に対して複製情報の再生を不許可にする。

【0052】ここで図2乃至図7を参照して本発明の第2実施形態に於ける動作を説明する。先ず、図3及び図4に示すフローチャートを参照して、暗号化及び復号化処理のための各種キー情報の設定処理を説明する。

【0053】再生指示に従うシステム起動に伴い、ドライブ装置40の暗号発生装置41はランダムな値をもとに暗号キー(1)を発生する(図3ステップ40a)。この暗号発生装置41より発生された暗号キー(1)はレジスタ42に保持されるとともに、CPU10の制御で再生装置60のレジスタ62にセットされる(図3ステップ10a、図4ステップ60a)。

【0054】又、再生装置60の暗号生成装置61もランダムな値をもとに暗号キー(2)を発生する(図4ステップ60b)。この暗号発生装置61より発生された暗号キー(2)はレジスタ63に保持されるとともに、CPU10の制御でドライブ装置40のレジスタ43にセットされる(図3ステップ10b、40b)。

【0055】ドライブ装置40の暗号生成装置44はレジスタ42に貯えられた暗号キー(1)とレジスタ43に貯えられた暗号キー(2)とを用いて暗号キー(3)を生成しレジスタ45にセットする(図3ステップ40c)。

【0056】又、再生装置60の暗号生成装置64はレジスタ62に貯えられた暗号キー(1)とレジスタ63に貯えられた暗号キー(2)とを用いて暗号キー(4)

を生成し、レジスタ65にセットする(図4ステップ60c)。

【0057】ドライブ装置40の読出装置46は情報記録媒体20より複製許可情報(CGMS)を読出し、レジスタ48にセットする(図3ステップ40d)。暗号化装置49は、レジスタ45に貯えられた暗号キー

(3)を用いて、レジスタ48にセットされた複製許可情報(CGMS)を暗号化処理する(図3ステップ40e)。この暗号化処理された複製許可情報(CGMS)はCPU10の制御で再生装置60の復号化装置66に渡

される(図3ステップ10c)。  
【0058】復号化装置66はレジスタ65に貯えられた暗号キー(4)を用いて、ドライブ装置40より受けた、暗号化処理されている複製許可情報(CGMS)を復号化処理し、レジスタ71にセットする(図4ステップ60d)。

【0059】再生装置60内の図示しない制御装置は、レジスタ71に貯えられた複製許可情報(CGMS)の内容を判断し、複製許可情報(CGMS)のb0、b1が“01”で、提供情報読出し時に利用された再生装置

のみに対して排他的な複製情報の再生を許可することを認識したとき、暗号化装置70を起動する(図4ステップ60e(Yes))。

【0060】これにより暗号化装置70はレジスタ65に貯えられた暗号キー(4)を用いて、レジスタ69に

固定的に貯えられている装置固有の提供情報暗号化キー(5)を暗号化処理する(図4ステップ60g)。  
【0061】又、複製許可情報(CGMS)のb0、b1が“01”でないときは、提供情報暗号化キー(5)に代わってダミーデータ(ヌル値)を生成する(図4ス

テップ60f)。  
【0062】CPU10は暗号化処理された装置固有の提供情報暗号化キー(5)又はそれに代わるダミーデータをドライブ装置40内の復号化装置50に転送する(図3ステップ10d)。

【0063】復号化装置50は再生装置60より受けた、暗号化処理された装置固有の提供情報暗号化キー(5)を復号化してレジスタ51にセットする。以上の処理により、暗号化及び復号化処理のための各種キー情報の設定処理が完了する。

【0064】次に、図5及び図6に示すフローチャートを参照して、提供情報読出し時に於ける複製制御処理を説明する。CPU10はドライブ装置40に対して提供情報の読出し指示を与える(図5ステップS1)。

【0065】ドライブ装置40内の図示しない制御装置は、CPU10より読出し指示を受けると、読出装置46が起動する。読出装置46は、情報記録媒体20をドライブ制御し、情報記録媒体20から提供情報(MPEG2データ)及び複製許可情報(CGMS)を読出す(図5ステップS2)。

【0066】情報記録媒体20から読出された複製許可情報(CGMS)はレジスタ48に貯えられた後、暗号化装置47に供給される。暗号化装置47は、レジスタ48に貯えられた複製許可情報(CGMS)の内容を判断し、CGMSのb0、b1が“00”であるとき、提供情報を暗号化処理せず、そのまま出力(パススルー)し、“01”であるとき、レジスタ51に貯えられた装置固有の提供情報暗号化キー(5)を用いて提供情報を暗号化処理し、“11”であるとき、レジスタ45に貯えられた暗号キー(3)を用いて提供情報を暗号化処理する(図5ステップS3～S7)。

【0067】この暗号化装置47より出力された提供情報(MPEG2データ)はシステムバス10Aを介して再生装置60内の復号化装置67に転送される(図5ステップS8)。

【0068】再生装置60の復号化装置67はドライブ装置40内の暗号化装置47より提供情報(MPEG2データ)を受けると、レジスタ71に貯えられた複製許可情報(CGMS)の内容を判断し、CGMSのb0、b1が“00”であるとき、提供情報を復号化処理せず、そのまま出力(パススルー)し、“01”であるとき、レジスタ72に貯えられた装置固有の提供情報暗号化キー(6)を用いて提供情報を復号化処理し、“11”であるとき、レジスタ65に貯えられた暗号キー(4)を用いて提供情報を復号化処理する(図5ステップS11～S16)。

【0069】この復号化装置67より出力された提供情報(MPEG2データ)はMPEG2デコーダ68によりデコード処理された後、表示コントローラ80に送られて表示装置81に表示出力される(図5ステップS17)。

【0070】この際、CPU10は、複製許可情報(CGMS)のb0、b1が“00”であるときは、提供情報(MPEG2データ)を記憶装置30に取り込むことによって、その複製情報を再生装置を特定せず任意に再生出力することができる。

【0071】又、複製許可情報(CGMS)のb0、b1が“01”であるときは、提供情報(MPEG2データ)を記憶装置30に取り込むことによって、暗号化処理に供された装置固有の提供情報暗号化キー(5)キーと対をなす装置固有の提供情報暗号化キー(6)をもつ再生装置60のみが複製情報を再生できる。

【0072】尚、この際、複製情報をレジスタ72に貯えられた暗号化キー(6)とともに、記憶装置30に保存しておくことにより、その後の再生処理でレジスタ72のキー値が書き替えられても、上記保存したキー情報を読出し、レジスタ72に再設定することで対応する複製情報の再生が可能となる。

【0073】又、複製許可情報(CGMS)のb0、b1が“11”であるときは、提供情報(MPEG2デー

10

20

30

40

50

タ)を複製情報として記憶装置30に取り込んでも、再生時に暗号キー(4)の値が既に変化していることから、その複製情報を復号化処理ができず、従って全ての再生装置に於いて複製情報を再生できない。

【0074】この際、複製許可情報(CGMS)の内容が切り替わる度に、それに同期してレジスタ69、72のキー値、又はレジスタ45、65のキー値を新たに設定する構成とすることにより、より信頼性の高い、任意情報量単位の緻密な許可制御を可能としたコピープロテクト機構が実現できる。

【0075】このように、情報提供側で、提供情報毎に(映画や音楽のタイトル毎に)暗号化を施すことができ、コンピュータなどで容易に情報を読み出せない構成としたことから、信頼性の高い、かつコンピュータ処理等による利用度の高い、提供情報の複製制御が確立される。

【0076】又、コンピュータなどで読み出された情報は、読み出し時に利用された情報再生装置のみでしか複製の再生できないようにすることができることから、複製情報の正当な利用を可能にし、不当な利用を排除できる。

【0077】上述したように本発明の実施形態によれば、大容量記録媒体等により提供される情報の受け渡しにコンピュータ装置が介在するシステムに於いても、コンピュータ装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能なシステムが構築できる。

【0078】尚、上記した実施形態では、情報提供媒体として、ドライブ装置を必要とするDVD、CD-ROM等の大容量ディスクを例に採ったが、情報提供媒体が例えば通信回線を介して外部に存在するシステム構成に於いても本発明を上記実施形態と同様に適用できる。この際は、図2に示すドライブ装置40内の読出装置46を除く各構成要素が通信先となる外部の情報提供装置に設けて、図2に破線で示す信号路を通信路に置き換えることで容易に実現できる。

【0079】又、上記した実施形態では、複製許可情報(CGMS)、及び装置固有の提供情報暗号化キー(5)をそれぞれ暗号化処理して転送しているが、必ずしも暗号化処理する必要はなく、要求される信頼性に応じて暗号化処理を省くことも可能である。

【0080】又、上記した第2実施形態では、ドライブ装置40及び再生装置60のそれぞれが、ランダムな情報をもとに一次キー情報を生成する構成としているが、これに限らず、例えば少なくともドライブ装置40又は再生装置60のいずれか一方が、ランダムな情報をもとに一次キー情報を生成し、当該キー情報をもとにしてドライブ装置40及び再生装置60がそれぞれ一時的

な二次キー情報を自己生成する構成等、要は、ドライブと情報再生装置がランダムな情報を用いて互いに関連するキー情報を一時的に生成する構成であればよい。

【0081】又、上記した実施形態では、再生装置60に於いて、装置固有の提供情報暗号化キー(5)と、装置固有の提供情報復号化キー(6)とをそれぞれ独立して設け、別個にレジスタ69、72に貯える構成としたが、これに限らず装置固有の提供情報暗号化キー(5)と復号化キー(6)とに共通のキー情報を用いてもよく、要は再生装置60が、入力された提供情報を復号化処理するために、入力された提供情報の暗号化方式と暗号化キーの内容を把握できればよい。

【0082】又、第2実施形態に於いては、暗号化処理に供された装置固有の提供情報暗号化キー(5)キーと対をなす装置固有の提供情報暗号化キー(6)をもつ再生装置60のみにより複製を再生できる、一世代コピーのみを許可する複製制御機構と、全ての再生装置に於いて複製の再生を不能にした複製制御機構とを選択的に用いる構成としているが、例えばコピーフリーの複製許可モードと、全ての再生装置に於いて複製の再生を不能にする複製許可モードとを選択する構成、又は、コピーフリーの複製許可モードと、一世代コピーの複製許可モードとを選択する構成等、任意の複製許可モードの組み合わせが可能である。

【0083】又、上記実施形態に於いては、大容量記録媒体、通信媒体等により提供される提供情報の受け渡しにコンピュータが介在するシステムを対象としているが、このシステム構成に拘らず、提供情報の受け渡しにコンピュータが直接介在しないシステム構成であっても、例えばMD、CD-ROM、DVD等の記録媒体より提供情報を読み取るドライブ又は提供情報の送信機能をもつ通信媒体と、その読み取りデータを再生する装置との間に於いて提供情報の複製が可能な装置間のインタフェース部分に於いて、上記実施形態に示す任意の複製制御機構を適用することができる。

【0084】又、この実施形態では、MPEG2により圧縮処理された映画、音楽等の提供情報を例に挙げたが、これに限らず、MPEG1又はMPEG4等により圧縮処理されたデータを含め再生対象とするシステム構成に於いても本発明を適用できる。

【0085】

【発明の効果】以上詳記したように本発明によれば、大容量記録媒体、通信媒体等により提供される提供情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステムに於いて、コンピュータ等の複製処理が可能な装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能な複製制御方法及び複製制御装置が提供できる。

## 【図面の簡単な説明】

【図 1】本発明の第 1 の実施形態に於ける基本的なシステム構成を示すブロック図。

【図 2】本発明の第 2 の実施形態に於けるシステム構成を示すブロック図。

【図 3】本発明の第 2 実施形態に於ける処理手順を示すフローチャート。

【図 4】本発明の第 2 実施形態に於ける処理手順を示すフローチャート。

【図 5】本発明の第 2 実施形態に於ける処理手順を示すフローチャート。

【図 6】本発明の第 2 実施形態に於ける処理手順を示すフローチャート。

【図 7】本発明の実施形態に於ける情報記録媒体 20 に記録されたメディア・ファイル管理情報ブロック内の複製許可情報 (CGMS) を説明するための情報フォーマットを示す図。

## 【符号の説明】

1…コンピュータ装置 (PC)

2…DVD (大容量記憶媒体)

\* 3…外部記憶装置

4…DVD ドライブ (ドライブ装置)

6…MPEG ボード (情報再生装置)

10…CPU

10A…システムバス

20…情報記録媒体

30…記憶装置

40…ドライブ装置

41, 44…暗号生成装置

42, 43, 45, 48, 51…レジスタ

46…読出装置

47, 49…暗号化装置

50…復号化装置

60…再生装置

61, 64…暗号生成装置

62, 63, 65, 69, 71, 72…レジスタ

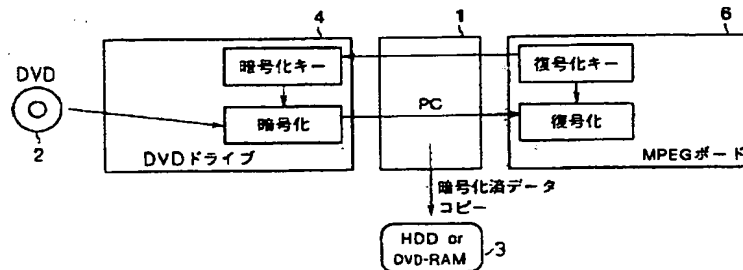
66, 67…復号化装置

68…MPEG 2 デコーダ

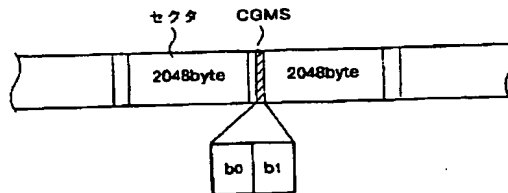
70…暗号化装置。

\* 20

【図 1】



【図 7】



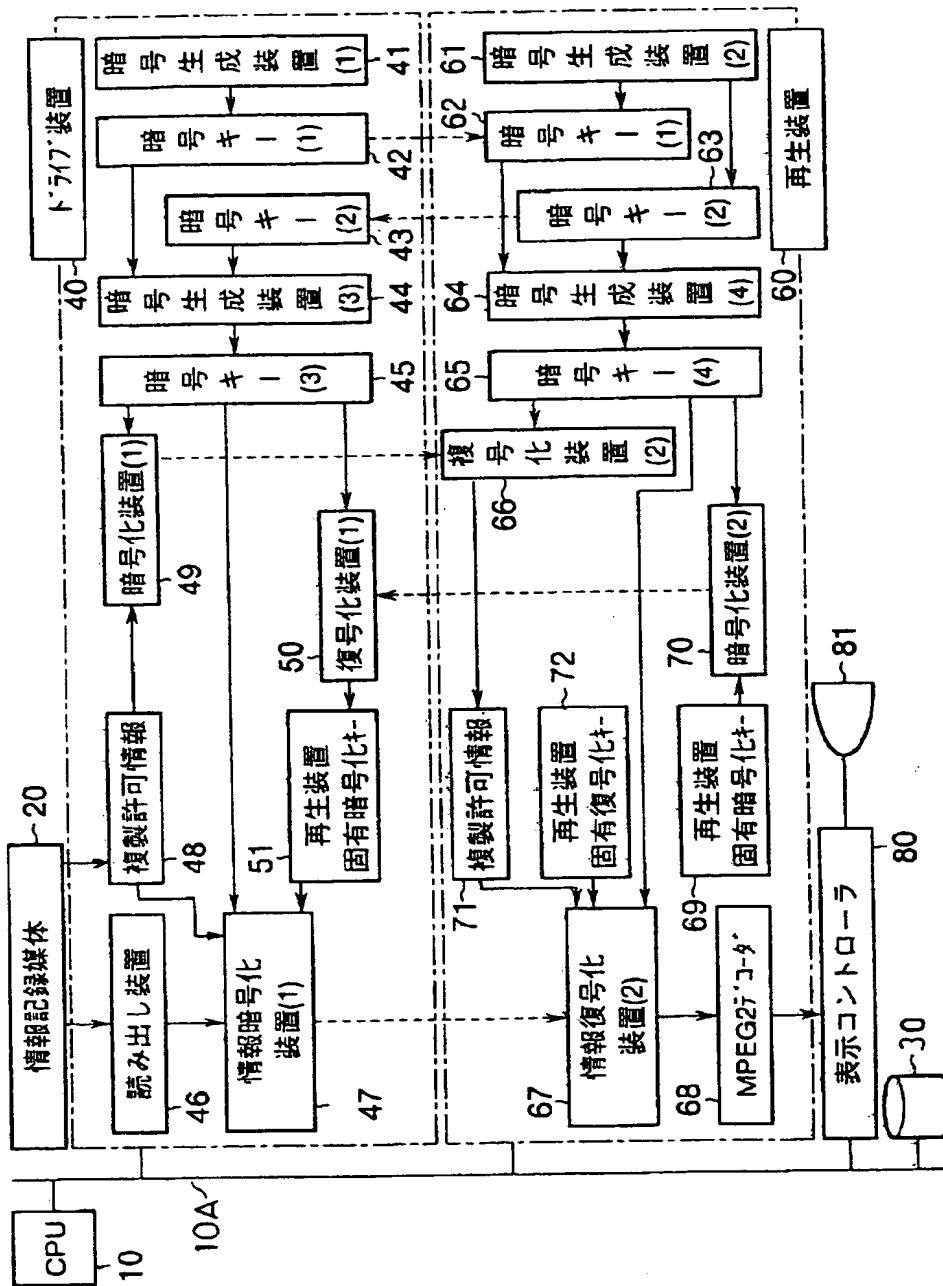
【CGMS】

b0, b1= "00" (複製の再生可)

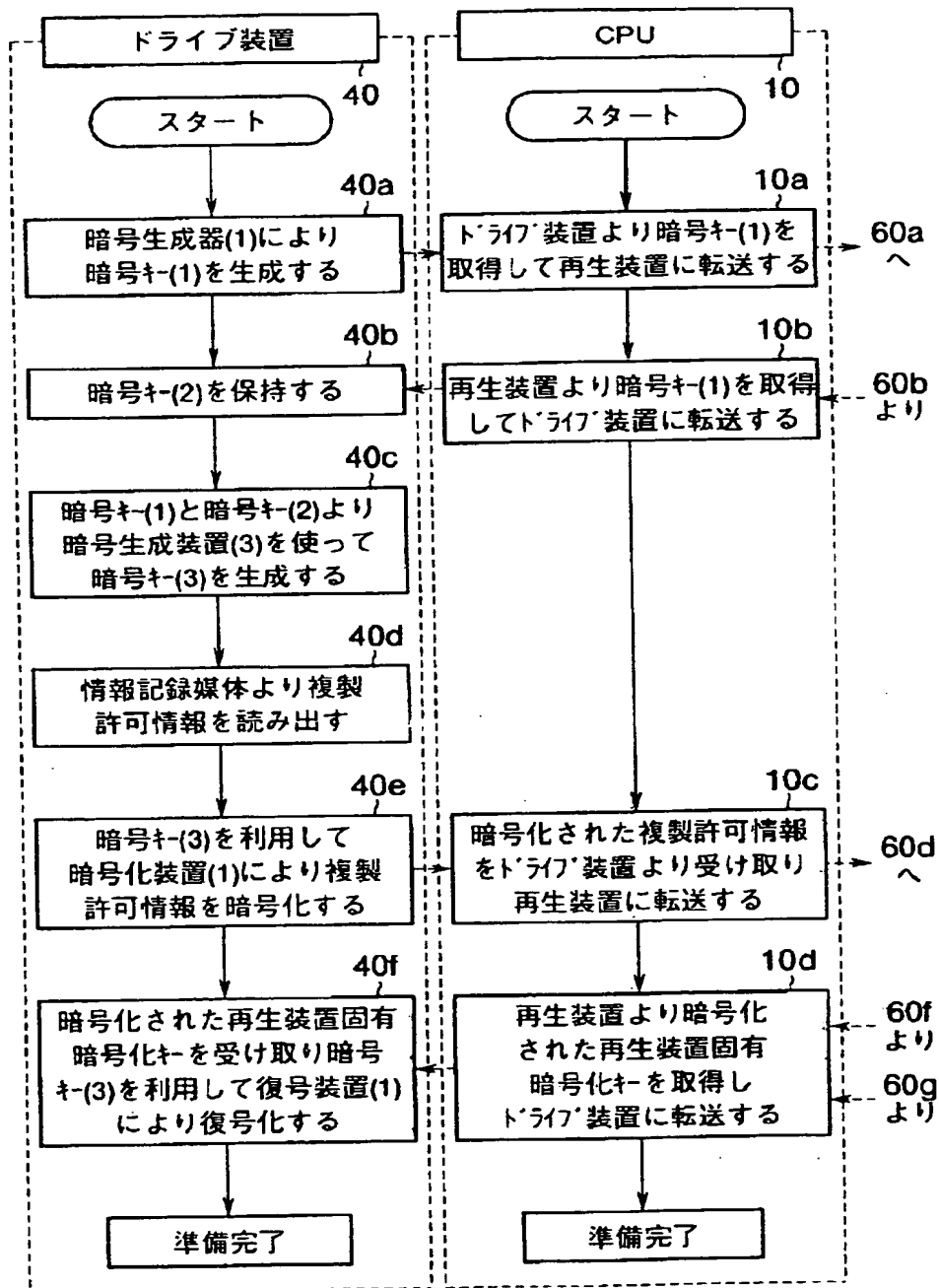
"01" (複製を作成したときに使用した装置でのみ複製の再生可)

"11" (複製の再生不可)

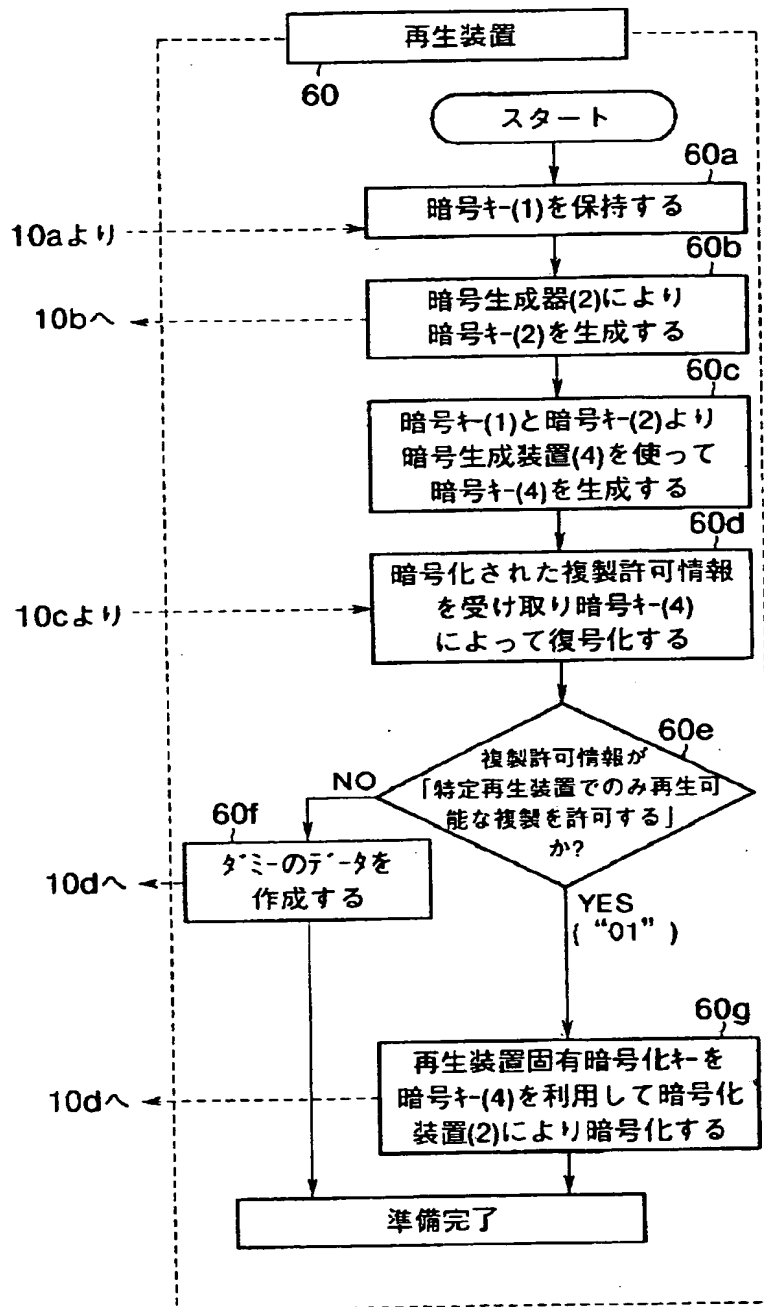
【図2】



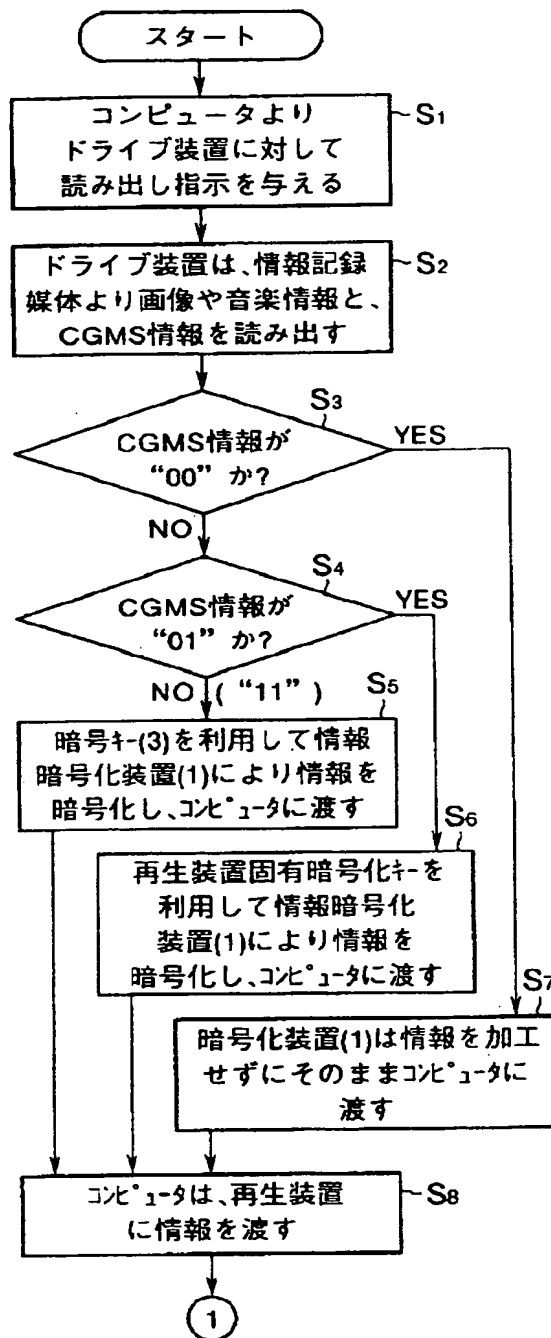
【図3】



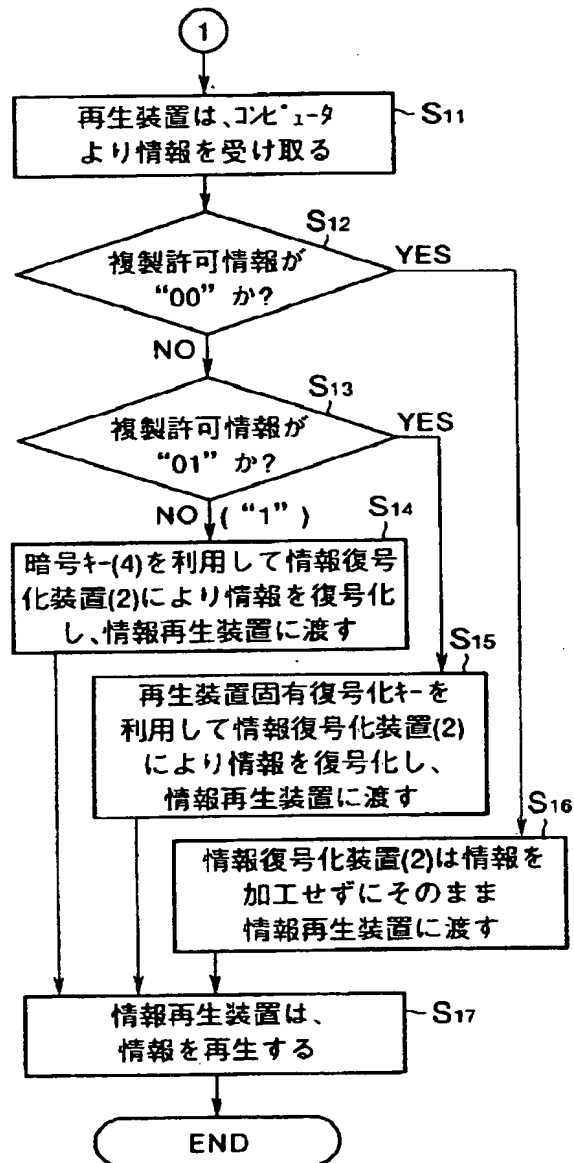
【図4】



【図5】



【図6】





【手続補正書】

【提出日】平成8年1月10日

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】請求項1

【補正方法】変更

【補正内容】

【請求項1】 大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備

えたシステムに於いて、

ドライブは、情報再生装置よりキー情報を受け、当該キー情報をもとに大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に渡し、

情報再生装置は、情報伝達手段から受けた暗号化処理された情報をドライブに発行したキー情報に関連するキー情報により復号化処理して再生できることを特徴とした大容量記録媒体に記録された情報の複製制御方法。

【公報種別】特許法第17条の2の規定による補正の掲載  
 【部門区分】第6部門第4区分  
 【発行日】平成13年4月6日(2001.4.6)

【公開番号】特開平9-190667  
 【公開日】平成9年7月22日(1997.7.22)  
 【年通号数】公開特許公報9-1907  
 【出願番号】特願平8-985  
 【国際特許分類第7版】

G11B 19/02 501

G06F 12/14 320

【F1】

G11B 19/02 501 Q

G06F 12/14 320 B

【手続補正書】

【提出日】平成12年4月25日(2000.4.25)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、

前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、

前記送信装置において少なくとも前記送信装置により読み出された複製制御情報と前記共通キーとを用いて前記情報を暗号化し、前記暗号化された情報と前記複製制御情報とを前記伝達手段を介して前記受信装置に転送するステップと、

前記受信装置において少なくとも前記伝達手段を介して受信した前記複製制御情報と前記共通キーとを用いて前記情報を復号化するステップとを具備することを特徴とする情報の複製制御方法。

【請求項2】前記生成ステップは、前記共通キーの為に少なくとも2種類の値を生成するステップを具備することを特徴とする請求項1記載の情報の複製制御方法。

【請求項3】前記暗号化ステップは、前記複製制御情報の値に従い、前記2種類の値のうちの一つを選択決定するステップを具備することを特徴とする請求項2記載の情報の複製制御方法。

【請求項4】前記生成ステップは、

前記送信装置において第1のランダム値に基づく第1のキーを生成するステップと、

前記受信装置において第2のランダム値に基づく第2のキーを生成するステップと、

前記送信装置と前記受信装置のそれぞれで生成した第1及び第2のキーを前記伝達手段を介して相互に交換するステップと、

前記相互に交換された第1及び第2のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する第1の共通キーを生成するステップとを具備することを特徴とする請求項3記載の情報の複製制御方法。

【請求項5】前記受信装置において第3のランダム値に基づく第3のキーを生成するステップと、

前記第1の共通キーを用いて、前記第3のキーを暗号化するステップと、

前記暗号化された第3のキーを前記受信装置から前記送信装置に転送し、前記送信装置と前記受信装置のそれぞれで保有する第2の共通キーを生成するステップとを更に具備することを特徴とする請求項4記載の情報の複製制御方法。

【請求項6】前記選択決定ステップは、前記複製制御情報が、複製の再生禁止を示している場合、前記共通キーの第1の値を選択決定するステップを具備することを特徴とする請求項5記載の情報の複製制御方法。

【請求項7】前記選択決定ステップは、前記複製制御情報が、複製を作成した時に使用した装置でのみ複製の再生可能を示している場合、前記共通キーの第2の値を選択決定するステップを具備することを特徴とする請求項5記載の情報の複製制御方法。

【請求項8】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、

前記送信装置において第1のランダム値に基づく第1のキーを生成するステップと、

前記送信装置において第2のランダム値に基づく第2のキーを生成するステップと、

前記送信装置と前記受信装置のそれぞれで生成した第1及び第2のキーを前記伝達手段を介して相互に交換する

ステップと、

前記相互に交換された第 1 及び第 2 のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、

前記送信装置と前記受信装置との間で転送される情報を保護する為の第 3 のキーを、前記送信装置と前記受信装置のいずれか一方の側で生成するステップと、

前記共通キーを用いて前記第 3 のキーを暗号化し、第 3 のキーが生成されていない装置側に前記暗号化された第 3 のキーを前記伝達手段を介して転送するステップと、前記暗号化された第 3 のキーを受信した装置側において前記共通キーを用いて前記暗号化された第 3 のキーを復号化するステップとを具備することを特徴とする情報の複製制御方法。

【請求項 9】前記第 3 のキーを生成するステップは、前記受信装置において前記第 3 のキーを生成するステップを具備することを特徴とする請求項 8 記載の情報の複製制御方法。

【請求項 10】前記第 3 のキーを生成するステップは、前記送信装置によって読み出される複製制御情報を生成するステップを具備することを特徴とする請求項 8 記載の情報の複製制御方法。

【請求項 11】前記第 1 のキーを生成するステップは、前記受信装置からの要求に応じて前記第 1 のキーを生成するステップを具備することを特徴とする請求項 8 記載の情報の複製制御方法。

【請求項 12】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、

前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、

前記送信装置において少なくとも前記送信装置により読み出された複製制御情報と前記共通キーとを用いて前記情報を暗号化する手段と、

前記暗号化された情報と前記複製制御情報とを前記伝達手段を介して前記受信装置に転送する手段と、

前記受信装置において少なくとも前記伝達手段を介して受信した前記複製制御情報と前記共通キーとを用いて前記情報を復号化する手段とを具備することを特徴とする情報の複製制御装置。

【請求項 13】前記生成手段は、前記共通キーの為に少なくとも 2 種類の値を生成する手段を具備することを特徴とする請求項 12 記載の情報の複製制御装置。

【請求項 14】前記暗号化手段は、前記複製制御情報の値に従い、前記 2 種類の値のうちの一つを選択決定する手段を具備することを特徴とする請求項 13 記載の情報の複製制御装置。

【請求項 15】前記生成手段は、

前記送信装置において第 1 のランダム値に基づく第 1 のキーを生成する手段と、

前記受信装置において第 2 のランダム値に基づく第 2 のキーを生成する手段と、

前記送信装置と前記受信装置のそれぞれで生成した第 1 及び第 2 のキーを前記伝達手段を介して相互に交換する手段と、

前記相互に交換された第 1 及び第 2 のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する第 1 の共通キーを生成する手段とを具備することを特徴とする請求項 14 記載の情報の複製制御装置。

【請求項 16】前記受信装置において第 3 のランダム値に基づく第 3 のキーを生成する手段と、

前記第 1 の共通キーを用いて、前記第 3 のキーを暗号化する手段と、

前記暗号化された第 3 のキーを前記受信装置から前記送信装置に転送し、前記送信装置と前記受信装置のそれぞれで保有する第 2 の共通キーを生成する手段とを更に具備することを特徴とする請求項 15 記載の情報の複製制御装置。

【請求項 17】前記選択決定手段は、前記複製制御情報が、複製の再生禁止を示している場合、前記共通キーの第 1 の値を選択決定する手段を具備することを特徴とする請求項 16 記載の情報の複製制御装置。

【請求項 18】前記選択決定手段は、前記複製制御情報が、複製を作成した時に使用した装置でのみ複製の再生可能を示している場合、前記共通キーの第 2 の値を選択決定する手段を具備することを特徴とする請求項 16 記載の情報の複製制御装置。

【請求項 19】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、

前記送信装置において第 1 のランダム値に基づく第 1 のキーを生成する手段と、

前記送信装置において第 2 のランダム値に基づく第 2 のキーを生成する手段と、

前記送信装置と前記受信装置のそれぞれで生成した第 1 及び第 2 のキーを前記伝達手段を介して相互に交換する手段と、

前記相互に交換された第 1 及び第 2 のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、

前記送信装置と前記受信装置との間で転送される情報を保護する為の第 3 のキーを、前記送信装置と前記受信装置のいずれか一方の側で生成する手段と、

前記共通キーを用いて前記第 3 のキーを暗号化し、第 3 のキーが生成されていない装置側に前記暗号化された第 3 のキーを前記伝達手段を介して転送する手段と、

前記暗号化された第 3 のキーを受信した装置側において前記共通キーを用いて前記暗号化された第 3 のキーを復号化する手段とを具備することを特徴とする情報の複製制御装置。

【請求項20】前記第3のキーを生成する手段は、前記受信装置において前記第3のキーを生成する手段を具備することを特徴とする請求項19記載の情報の複製制御装置。

【請求項21】前記第3のキーを生成する手段は、前記送信装置によって読み出される複製制御情報を生成する手段を具備することを特徴とする請求項19記載の情報の複製制御装置。

【請求項22】前記第1のキーを生成する手段は、前記受信装置からの要求に応じて前記第1のキーを生成する手段を具備することを特徴とする請求項19記載の情報の複製制御装置。

【請求項23】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、

前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、

前記送信装置において少なくとも前記共通キーを用いて前記送信装置により読み出される複製制御情報を暗号化し、前記暗号化された複製制御情報を前記伝達手段を介して前記受信装置に転送するステップと、

前記受信装置において少なくとも前記共通キーを用いて前記伝達手段を介して受信した前記複製制御情報を復号化するステップとを具備することを特徴とする情報の複製制御方法。

【請求項24】前記生成ステップは、前記送信装置において第1のランダム値に基づく第1のキーを生成するステップと、

前記受信装置において第2のランダム値に基づく第2のキーを生成するステップと、

前記送信装置と前記受信装置のそれぞれで生成した第1及び第2のキーを前記伝達手段を介して相互に交換するステップと、

前記相互に交換された第1及び第2のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する第1の共通キーを生成するステップとを具備することを特徴とする請求項23記載の情報の複製制御方法。

【請求項25】前記選択決定ステップは、前記複製制御情報が、複製の再生禁止を示している場合、前記共通キーの第1の値を選択決定するステップを具備することを特徴とする請求項24記載の情報の複製制御方法。

【請求項26】前記受信装置において第3のランダム値に基づく第3のキーを生成するステップと、前記第1の共通キーを用いて、前記第3のキーを暗号化するステップと、

前記暗号化された第3のキーを前記受信装置から前記送信装置に転送し、前記送信装置と前記受信装置のそれぞれで保有する第2の共通キーを生成するステップとを更に具備することを特徴とする請求項24記載の情報の複製制御方法。

【請求項27】前記選択決定ステップは、前記複製制御情報が、複製を作成した時に使用した装置でのみ複製の再生可能を示している場合、前記共通キーの第2の値を選択決定するステップを具備することを特徴とする請求項26記載の情報の複製制御方法。

【請求項28】送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、

前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、

前記送信装置において少なくとも前記共通キーを用いて前記送信装置により読み出される複製制御情報を暗号化し、前記暗号化された複製制御情報を前記伝達手段を介して前記受信装置に転送する手段と、

前記受信装置において少なくとも前記共通キーを用いて前記伝達手段を介して受信した前記複製制御情報を復号化する手段とを具備することを特徴とする情報の複製制御装置。

【請求項29】前記生成手段は、

前記送信装置において第1のランダム値に基づく第1のキーを生成する手段と、

前記受信装置において第2のランダム値に基づく第2のキーを生成する手段と、

前記送信装置と前記受信装置のそれぞれで生成した第1及び第2のキーを前記伝達手段を介して相互に交換する手段と、

前記相互に交換された第1及び第2のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する第1の共通キーを生成する手段とを具備することを特徴とする請求項28記載の情報の複製制御装置。

【請求項30】前記選択決定手段は、前記複製制御情報が、複製の再生禁止を示している場合、前記共通キーの第1の値を選択決定する手段を具備することを特徴とする請求項29記載の情報の複製制御装置。

【請求項31】前記受信装置において第3のランダム値に基づく第3のキーを生成する手段と、

前記第1の共通キーを用いて、前記第3のキーを暗号化する手段と、

前記暗号化された第3のキーを前記受信装置から前記送信装置に転送し、前記送信装置と前記受信装置のそれぞれで保有する第2の共通キーを生成する手段とを更に具備することを特徴とする請求項29記載の情報の複製制御装置。

【請求項32】前記選択決定手段は、前記複製制御情報が、複製を作成した時に使用した装置でのみ複製の再生可能を示している場合、前記共通キーの第2の値を選択決定する手段を具備することを特徴とする請求項31記載の情報の複製制御装置。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】変更

【補正内容】

【0014】本発明に係る情報の複製制御方法は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、前記送信装置において少なくとも前記送信装置により読み出された複製制御情報と前記共通キーとを用いて前記情報を暗号化し、前記暗号化された情報と前記複製制御情報とを前記伝達手段を介して前記受信装置に転送するステップと、前記受信装置において少なくとも前記伝達手段を介して受信した前記複製制御情報と前記共通キーとを用いて前記情報を復号化するステップとを具備することを特徴とする。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0015

【補正方法】変更

【補正内容】

【0015】また、本発明に係る情報の複製制御方法は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、前記送信装置において第1のランダム値に基づく第1のキーを生成するステップと、前記送信装置において第2のランダム値に基づく第2のキーを生成するステップと、前記送信装置と前記受信装置のそれぞれで生成した第1及び第2のキーを前記伝達手段を介して相互に交換するステップと、前記相互に交換された第1及び第2のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、前記送信装置と前記受信装置との間で転送される情報を保護する為の第3のキーを、前記送信装置と前記受信装置のいずれか一方の側で生成するステップと、前記共通キーを用いて前記第3のキーを暗号化し、第3のキーが生成されていない装置側に前記暗号化された第3のキーを前記伝達手段を介して転送するステップと、前記暗号化された第3のキーを受信した装置側において前記共通キーを用いて前記暗号化された第3のキーを復号化するステップとを具備することを特徴とする。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

【補正内容】

【0016】また、本発明に係る情報の複製制御装置は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、前記送信装置と前記受信装置

のそれぞれで保有する共通キーを生成する手段と、前記送信装置において少なくとも前記送信装置により読み出された複製制御情報と前記共通キーとを用いて前記情報を暗号化する手段と、前記暗号化された情報と前記複製制御情報とを前記伝達手段を介して前記受信装置に転送する手段と、前記受信装置において少なくとも前記伝達手段を介して受信した前記複製制御情報と前記共通キーとを用いて前記情報を復号化する手段とを具備することを特徴とする。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】変更

【補正内容】

【0017】また、本発明に係る情報の複製制御装置は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御装置であって、前記送信装置において第1のランダム値に基づく第1のキーを生成する手段と、前記送信装置において第2のランダム値に基づく第2のキーを生成する手段と、前記送信装置と前記受信装置のそれぞれで生成した第1及び第2のキーを前記伝達手段を介して相互に交換する手段と、前記相互に交換された第1及び第2のキーを用いて、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、前記送信装置と前記受信装置との間で転送される情報を保護する為の第3のキーを、前記送信装置と前記受信装置のいずれか一方の側で生成する手段と、前記共通キーを用いて前記第3のキーを暗号化し、第3のキーが生成されていない装置側に前記暗号化された第3のキーを前記伝達手段を介して転送する手段と、前記暗号化された第3のキーを受信した装置側において前記共通キーを用いて前記暗号化された第3のキーを復号化する手段とを具備することを特徴とする。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正内容】

【0018】また、本発明に係る情報の複製制御方法は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報の複製制御方法であって、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成するステップと、前記送信装置において少なくとも前記共通キーを用いて前記送信装置により読み出される複製制御情報を暗号化し、前記暗号化された複製制御情報を前記伝達手段を介して前記受信装置に転送するステップと、前記受信装置において少なくとも前記共通キーを用いて前記伝達手段を介して受信した前記複製制御情報を復号化するステッ

ブとを具備することを特徴とする。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0 0 1 9

【補正方法】変更

【補正内容】

【0 0 1 9】また、本発明に係る情報の複製制御装置は、送信装置により読み出された情報を伝達手段を介して受信する受信装置を備えたシステムに適用される情報

の複製制御装置であって、前記送信装置と前記受信装置のそれぞれで保有する共通キーを生成する手段と、前記送信装置において少なくとも前記共通キーを用いて前記送信装置により読み出される複製制御情報を暗号化し、前記暗号化された複製制御情報を前記伝達手段を介して前記受信装置に転送する手段と、前記受信装置において少なくとも前記共通キーを用いて前記伝達手段を介して受信した前記複製制御情報を復号化する手段とを具備することを特徴とする。